Testimony of

Alan Paller, Director of Research, The SANS Institute

Before the

House Committee on Homeland Security
Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity

Hearings on SCADA and the Terrorist Threat: Protecting the Nation's Critical Control Systems

October 18, 2005

Thank you for your leadership, Mr. Chairman and Madam Ranking Member, in shining a bright light on the insecurity of SCADA systems, illuminating the threat to the nation posed by their increasingly troublesome vulnerabilities.

My testimony today focuses on what can be done, quickly, economically and without new laws or regulations, to protect SCADA systems from attack. I'll do that in four steps:

1. Providing specific examples of the damage that has already been done by attacks on industrial control systems
2. Detailing why SCADA security is getting worse, not better.
3. Summarizing the available evidence on terrorist's use of cyber crime and how that can involve SCADA systems
4. Describing a promising and economical approach to improving SCADA security, an approach that has already been proven to work.

About the SANS Institute

The SANS Institute is the educational institution that prepares technical security professionals for positions of responsibility in protecting information systems. Our 47,000 alumni manage information security for commercial, government, and academic organizations throughout the world. At SANS they go through immersion training in intrusion detection, cyber forensics, perimeter protection, blocking hacker exploits, network and system security auditing, and security leadership. Courses range from foundational to the most advanced programs available anywhere in the world. SANS Institute faculty members exhibit two characteristics that set them apart from other security professionals: (1) They have the practical, in-the-trenches knowledge that makes their teaching credible. For example, SANS faculty have held positions as the Information Warfare Officer for the US Ballistic Missile Defense Organization, the internal Red Team Leader for the CIA, and the Technical Director for the Department of Defense Joint Task Force on Computer Network Operations. (2) They are the winners of an eleven-year competition designed to identify the best teachers in the security field. More than 700 people have tried out for positions on the SANS faculty; fewer than 30 have been selected.

We also manage major research initiatives designed to enable our alumni to maintain their knowledge and skills after they complete SNAS training, and to help them protect their employers' information systems in the face of a constantly changing threat. For example, SANS operates the Internet Storm Center – the early warning system for the Internet with 6,000 sensors all over the world. It was Storm Center that discovered and illuminated the Leaves worm, the Lion worm, and the Katrina fund-raising web sites scams and it is Storm Center that security professionals look to every morning to learn what new attacks were launched overnight. SANS also publishes weekly security newsletters including summaries of all newly discovered security vulnerabilities with suggested solutions. That information is all available at no cost to our alumni and to every other person engaged in information security around the world. (www.sans.org)

Real Damage Has Resulted From SCADA Problems and Attacks

On October 31, 2001, Vitek Boden, an Australian, was sentenced to two years in prison for hacking into the SCADA system that controlled the sewage treatment plant in Maroochy Shire in Queensland, Australia.

Boden changed valve settings causing raw sewage to back up on the streets of the city, on the grounds of the local Hyatt Regency hotel (picture) and into the rivers. An Australian Environmental Protection official said, "Marine life died, the river turned black, the stench was unbearable for residents." And that was just sewage.

An event in January 2003 illustrated how accessible and vulnerable SCADA systems are at nuclear power plants, because they rely on vulnerable Microsoft operating systems, and why most utility executives are unaware of the risk. That month a computer worm, called SQL Slammer (SQL is a popular Microsoft data base management system), was circulating on the Internet. The Davis-Besse nuclear power plant, managed by FirstEnergy, had a firewall that blocked Internet traffic using SQL Slammer's path. Sadly, according to reports filed by FirstEnergy with the Nuclear Regulatory Commission (NRC), a Davis-Besse contractor had not protected that contractor's network. The worm came into the contractor's network, passed down a T1 communications line to the Davis-Besse computers without going through the firewall, and infected Davis-Besse business systems. Because of Davis-Besse's widespread use of vulnerable Microsoft software, the worm jumped to the plant network and crashed the Safety Parameter Display Systems, keeping it offline for eight hours. The report to NRC said "Some people in [First Energy's] Network Services department were aware of this T1 connection and some were not."

Because the Davis-Besse plant was offline and because it had back-up safety systems, this specific outage did not pose a major risk to public safety. However, the practices of using unprotected Windows operating systems and allowing contractors to bypass the firewall are common; many power plants and other elements of the critical infrastructure have similar vulnerabilities.

The bottom line is that real damage has already been done at some locations where SCADA systems are in use, and that the defenses SCADA operators have put in place can no longer be counted on to stop the attacks.

The Problem Is Getting Worse

In March 2004, the Government Accountability Office (GAO) published a report on SCADA security that it produced at the request of the House Committee on Government Reform Subcommittee on Technology and Information Policy. That report focused, in part, on why the risk to SCADA systems is increasing. It listed the four factors contributing to the escalation of risk to SCADA systems:

1. Control systems are adopting standardized technologies with known vulnerabilities. Essentially this means Microsoft software, UNIX and Linux software, and the Internet. The Davis-Besse example showed how reliance on Microsoft software and on the Internet enable malicious programs to take over utility control systems.
2. Control systems are connected to other networks that are not secure. This, too, was illustrated in the Davis-Besse outage, but we'll see an example of this in a moment.
3. Insecure connections exacerbate vulnerabilities. GAO focused on dial up connections, but the Davis-Besse worm attack illustrated that Internet connections are also insecure.
4. Manuals on how to use SCADA systems are publicly available to the terrorists as well as to legitimate users.

The event that first persuaded me that SCADA systems are directly vulnerable to terrorists and that real damage can be done, was documented in a book called @Large. It is ancient history now, having occurred in the early 1990s, but it is a perfect model for the attacks of today. It also helps explain the increasing vulnerability GAO described in its report.

Forty years ago, dam control rooms looked like the picture at the left, but over the next decades most of those manual systems were replaced by computerized control systems.

While this transition was taking place, particularly in the seventies and eighties, American's became aware of the possibility that terrorists could take control of the dams and open the spillway gates – flooding cities and killing people. Government officials, faced with the threat of such a catastrophic event, looked for a way to protect the citizens from such an attack.

Computer networks were new and seemed promising. Some government officials decided to build communications links from their computers to the control systems at the dams so that officials could override any action a terrorist might take from inside the dam's control room.

Sadly, their actions created a new vulnerability much larger than the one they were trying to solve. Their error was documented by the authors of @Large. The authors described an FBI investigation of a hacker who had broken into many government systems. The lead FBI agent, Brent Rasmussen, discovered that the hacker had penetrated a Department of Interior network in Portland, OR, roamed that agency's national network, and skipped to Sacramento, "where he easily obtained root access on the computers that controlled every dam in the northern part of the state [of California]."

Root access means total control. The hacker could enter exactly the same override commands that the government planned to use to thwart terrorists. This particular hacker was just exploring every computer he could take over and had no knowledge of the dams he could control. The lack of effective security on the government systems and their ability to control the dam's spillways combine to offer a chilling roadmap for people who want to do harm to the United States.

So if the threat is real and it is getting worse, one must ask how and where terrorists can be expected to exploit these vulnerabilities.

Are Terrorists Using Cyber Crime?

Imam Samudra (picture) is the "first" Bali Bomber, the Al Qaeda chief who purchased and planted the bombs that killed more than 200 tourists in Bali in 2003. He was convicted and is now on death row.

Forensic analysis of Samudra's laptop uncovered evidence that the terrorist was involved in hacking for profit through credit card fraud. While on death row, Samudra wrote his autobiography and had it published by a commercial publisher in Indonesia. One of the chapters, called "Hacking, Why Not?" provided step-by-step guidance for his followers on how to become competent hackers and told his readers why he wanted Al Qaeda members to become hackers, saying,

> **"If hacking is successful, get ready to gain windfall income for just 3 to 6 hours of work, greater than the income a policeman earns in 6 months of work. But, please do not do that for money alone! I want to motivate the youth and Moslem men who are granted perfect mind by Allah; I want America and its cronies to be crushed in all aspects."**

Terrorist are getting better at hacking computers to raise money, and can be expected to add cyber extortion to their portfolio of crimes. SCADA systems can be a potent target for them.

Dave Thomas, chief of the FBI's Computer Intrusion Section, reports that the FBI is receiving more than one new case of cyber extortion every day. Criminals hack into computers and then threaten to expose or change information or disable the computers if the victims do not pay. Most victims are online businesses, but an extortion involving a computer that controlled a life-support system provides an example of cyber extortion more relevant to today's hearing.

In January 2003, a Romanian pair hacked into the computers at the Amundsen-Scott South Pole Station that controlled the life support for the 50 scientists there. The attackers demanded money. This attack suggests a future scenario in which a compromised SCADA system at a nuclear power station could lead to substantial extortion demands and more money for terrorism.

In sum, SCADA systems are vulnerable, their compromises have caused real damage and can cause much more, and the attackers don't have to be experts in SCADA operations to use SCADA compromises to extort money from operators of information systems controlling the critical infrastructure.

Is There A Cost-Effective Solution?

Surprisingly, there is an effective approach, that does not require regulation or legislation, and that has already been proven to be effective by the US Air Force. It recognizes the futility and waste of asking every buyer of SCADA technology to learn to reconfigure their SCADA systems for security, when the SCADA vendors can do that job one time and do it cost effectively. This approach employs the buying power of the users to persuade the vendors to do the work.. In the biggest example of the technique, the Air Force said to Microsoft, we will buy 525,000 Windows systems, if you are willing to sell them to us safely configured. Microsoft is to be applauded. The company said yes.

Procurement leverage is effective because it places the responsibility for securing systems in the only place that security tasks can be done cost effectively – in the hands of the system vendor that created the systems. The vendor is the only organization that knows the technology well enough to know how it can be secured, and the vendor can do it one time on behalf of all users. If, instead, you try to force every user to secure their systems, every user would have to study every system they buy and become a security expert on every system, and then they would do the same job the vendor could have done one time. Allowing vendors to foist the security configuration job onto their users is what got us into this vulnerable status. That's what has to change. That's what the Air Force changed by leveraging its Windows procurement. That's what government leadership can change by leveraging SCADA procurements.

The Air Force consolidated 38 contracts, creating a single, six year, $500 million procurement of Windows operating system and application software for 525,000 Air Force computers. Procurement consolidation allowed the Air Force to pay $100 million less than they would have paid had they not consolidated their buying. The main purpose of the procurement, however, was improved security. The Air Force required the software vendors to deliver Windows software pre-configured securely, so that every Air Force base didn't have to reconfigure it. Nearly every other buyer of Windows systems has to do the reconfiguration themselves, and few do it well.

The Air Force contract offers continuing savings and better long term security, because the standard configurations they are buying can be patched automatically and quickly. Automatic patching saves money. Quick patching protects Air Force systems from attacks other organizations face.

One critical element of the Air Force's procurement illuminates what DHS can do to improve security of SCADA systems. The Air Force had to have detailed security configuration standards to put in the Windows procurement. Without those specifications, there would be no standardization, and the entire secure Windows initiative would have faltered. The Air Force relied on secure configuration standards developed by the Center for Internet Security and the US National Security Agency.

What is not well known about the Air Force procurement was the role played by the Department of Homeland Security. DHS provided partial funding for the Center for Internet Security – the organization that created the consensus security specifications used in the Air Force procurement. The Center for Internet Security is a not-for-profit association of private and public technology users who combine their knowledge of security vulnerabilities in products they buy. The members of the Center build consensus specifications for securing more than a dozen common systems- including the operating systems commonly employed in modern SCADA systems. The Center's work is, in my opinion, the single greatest contribution DHS has made to meeting its published goal of reducing security vulnerabilities of the nation's critical cyber infrastructure. It is also the best example of a public-private partnership that actually improves security.

This same technique can be put to work in improving SCADA security and DHS has a central role.

First, DHS and the Center for Internet Security can bring together the SCADA vulnerability research that has been spearheaded by the extraordinary people at Sandia National Laboratory and the Idaho National Laboratory, with the experience of other users of SCADA equipment, to develop consensus safe configuration benchmarks for SCADA systems, very quickly. Once those configuration benchmarks are set, buyers of SCADA systems inside the government can incorporate those safe configuration benchmarks in their SCADA procurement documents. SCADA vendors that want their business will see their economic interest lies in meeting the requirement for safer SCADA systems. Non government buyers can also use the consensus specifications.

Sadly, what I just described, even if 100% successful, will still leave most of the critical infrastructure vulnerable for many years, because insecure SCADA system have very long lives. SCADA systems usually last ten to fifteen years and many last longer. To protect the legacy SCADA systems, a parallel technique can be used. SCADA vendors charge substantial maintenance fees, and buyers pay those fees. As part of the renegotiation of annual maintenance fees, the vendors can be persuaded to develop and deliver special network filters that isolate the legacy SCADA systems from other parts of the network – allowing only very specific information in very limited formats to get to or from the SCADA systems and to get to or from the systems that manage the SCADA systems. Only the SCADA vendors know what parts of the

network traffic are essential and what parts can be blocked. Here again, expertise from INEL and Sandia can help enable the process.

This second technique – filtering legacy systems – is the only known solution for securing old SCADA systems that use operating systems that cannot be patched and is a second layer of defense that can help protect even securely configured SCADA systems.

Here's the bottom line: We can improve security on SCADA systems quickly through DHS leadership and intelligent use of federal procurement. The costs are low; the value is high. We owe it to the country to try.

The Air Force demonstrates that safer systems can be acquired at very low additional costs. The vendors decided to comply because they wanted the $500 million dollars the Air Force would spend if they did. That $500 million (over 6 years) accounts for about one tenth of one percent of federal IT spending. Yet it has had a huge impact. Already Microsoft's Director of Security Engineering Strategy, Steve Lipner, told a Department of Energy cybersecurity conference audience in April 2005 that the next step for Microsoft, after the Air Force deal, is to "deliver the safer systems to all our customers."

If changing the specifications in one procurement, involving one tenth of one percent of the Federal IT budget could have that impact, think what can be done with a larger share of the IT budget. How many IT suppliers, including SCADA vendors, could be persuaded to deliver safer systems?

I greatly appreciate your allowing me to meet with you today and I look forward to your questions.